

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
22 February 2001 (22.02.2001)

PCT

(10) International Publication Number
WO 01/13666 A1

(51) International Patent Classification¹:

H04Q 7/38

(81) Designated States (national): AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(21) International Application Number: PCT/FI00/00691

(22) International Filing Date: 15 August 2000 (15.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

19991733 16 August 1999 (16.08.1999) FI

(71) Applicant (for all designated States except US): NOKIA NETWORKS OY [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(84) Designated States (regional): ARPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

(72) Inventor; and

(75) Inventor/Applicant (for US only): STENBERG, Timo [FI/FI]; Löylyspolku 2 C 39, FIN-01600 Vantaa (FI).

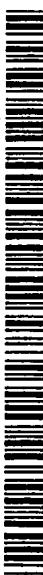
(74) Agent: KOLSTER OY AB; Iso Roobertinkatu 23, P.O. Box 148, FIN-00121 Helsinki (FI).

Published:

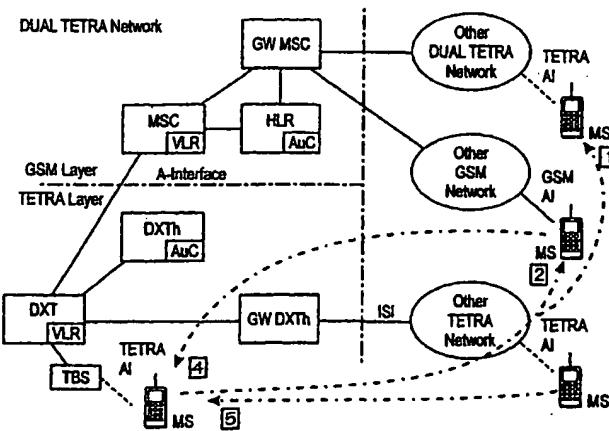
— With international search report.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: AUTHENTICATION IN A MOBILE COMMUNICATIONS SYSTEM



A1



(57) Abstract: In the present invention a radio access network infrastructure, such as the TETRA, is connected to a second network infrastructure, such as a network sub-system (NSS) of the GSM, which has different authentication procedures and triplets than the radio access network. The problem relating to the different authentication schemes is overcome by using the authentication of the overlaying network layer in combination with the authentication procedures of the radio access network layer. When the mobile station (MS) registers to the system, the mobile station is first authenticated in the overlaying network layer (GSM). In this initial authentication the authentication procedures and authentication parameters of the overlaying network, such as the authentication triplet of the GSM, is used. The authentication parameters of the radio access layer (TETRA), such as the random seed and the random challenge of the TETRA, are derived from the authentication parameters used in the initial authentication. Then the derived authentication parameters are used in any subsequent authentication procedure within the first radio access infrastructure layer (TETRA) until a new authentication is needed in the overlaying network infrastructure layer (GSM).

WO 01/13666 A1

Authentication in a mobile communications system

Field of the invention

The invention relates to authentication in a mobile communications system, and particularly in a system comprising an access network with a first authentication procedure and an overlaying network with a second authentication procedure.

Background of the invention

A mobile communications system refers generally to any telecommunications system which enables wireless communication when users are moving within the service area of the system. A typical mobile communications system is a Public Land Mobile Network (PLMN). Often the mobile communications network is an access network providing a user with a wireless access to external networks, host, or services offered by specific service providers.

TETRA (Trans-European Trunked Radio) is a standard defined by ETSI (European Telecommunications Standards Institute) for digital professional mobile radio or private mobile radio (PMR) systems. The TETRA system is developed primarily for professional and governmental users, such as police, military forces, oil plants, etc.

In any radio system both the users and the operators should be protected against an undesired intrusion by third parties, whether the intrusion is intentional or not. For example, an illegal access to the network can be prevented by authentication of the mobile station by the network. The risk of eavesdropping can be decreased by use of encryption.

Authentication is a procedure where a party authenticates the other according to an agreed procedure. This is normally based on a common secret which both parties know and compare. As transferring of this secret on the radio path itself presents a security risk, the basic principle is that the authentication information on the radio path is changed each time according a secret algorithm. In the TETRA, the authentication can be divided into authentication of the mobile station by the network in order to prevent illegal access to the network, and authentication of the network by a mobile station in order to prevent the radios from roaming into a fake TETRA system. The authentication of the mobile station is familiar from cellular networks like the GSM (Global System for Mobile Communication), but the authentication of the network by a mobile station is a TETRA-specific feature. The authentication is performed

when a radio registers into the system or at the request of the network. The authentication key is stored in the authenticating parties which are the authentication center AuC in the infrastructure and the mobile station MS. The standard TETRA authentication of the user by the infrastructure is illustrated in

5 Figure 1. The secret, the authentication key K, is stored both in the authentication center and in the MS (e.g. in subscriber identification module SIM). The authentication center AuC of the home system of the MS generates a random number (random seed RS), and thereafter carries out a computation of the session authentication key KS by an algorithm TA11 having the inputs K and

10 RS. The authentication center AuC forwards the pair of RS and KS parameters to the base station BS. The base station BS generates a random number as a challenge RAND1 and sends a pair of parameters RAND1 and RS to the MS. The MS derives the session authentication key KS from the authentication key K and the received random seed RS by the algorithm TA11. Thereafter,

15 the MS computes a response RES1 from the session authentication key KS and the received challenge RAND1 by an algorithm TA12 which at the same time produces a derived cipher key DCK1. The MS sends the response RES1 to the BS. The BS will also compute an expected response XRES1 from the challenge RAND1 and the session authentication key KS by the algorithm

20 TA12, also producing the DCK1. The derived cipher key DCK is used by an encryption algorithm for encryption of individual calls. On receipt of the RES1 from the MS, the BS compares it with the XRES1. If the values are equal (i.e. the MS employs the correct authentication key K), the authentication is successful and the result R1 is set to TRUE. If the values are not equal, the MS is

25 not a correct one and the result R1 is set to FALSE.

Authentication of the infrastructure by a user is carried out in the same way except that the roles of the MS and the BS are changed, as illustrated in Figure 2. The MS generates a random number as a challenge as well as an expected response XRES2, and sends the RAND2 to the BS. The

30 BS generates the response RES2 and returns it to the MS. The derived cipher key DCK2 is also generated at the MS and the BS. On receipt of the RES2 from the BS, the MS compares it with the XRES2. If the values are equal the result R2 will indicate that the authentication is successful, otherwise the result R2 will indicate that the authentication has failed. The same authentication key

35 K is used as in the case of authentication of the user by the infrastructure in Figure 2 together with a random seed RS.

It is also possible to carry out a mutual authentication of user and infrastructure, in which the above procedures are performed in parallel as illustrated in Figure 3

The TETRA authentication procedures and algorithms differ from those of the GSM. The size and the content of authentication triplets are different, too. In the GSM each authentication requires a triplet from the authentication center AuC. In the TETRA the authentication has two phases: 1) the BS gets a triplet from the AuC, and 2) the BS authenticates the MS using this triplet once or several times. These differences prevent dual (or multi) mode mobile stations MS which have both the GSM and TETRA capability from roaming from the TETRA to the GSM, and vice versa. When a mobile station roams into another network, the authentication information from the home network of the MS must be transferred to the visited network. The visited network has to be somehow connected to the home network. The visited network or the MS or both have to adapt their authentication methods, so that a successful authentication can be performed.

Moreover, TETRA networks will also have to support many of the new services and features which are or will be available in the GSM or the third-generation mobile systems, such as UMTS. The development of the features and services for the TETRA will be an enormous task and therefore it would be more convenient and economical if at least some of the development work already done in the other systems can also be used in the TETRA system.

One approach considered by the present inventor is a new dual TETRA network architecture which consists of a TETRA network layer operating as an access network and an overlaying GSM network layer. The TETRA layer provides all the TETRA-specific features of the system. The overlaying GSM layer which is connected to the TETRA layer via an A-interface provides the GSM-specific services available to the mobile stations MS via the TETRA layer. In a similar manner the overlaying network layer could be GPRS (General Packet Radio Service) or any other core network. Such a combination of TETRA and GSM networks allows the subscribers to roam in both networks and enables the TETRA network to use some of the GSM features and services. However, the authentication problems described above due to the different authentication procedures of the GSM and the TETRA are encountered also in the dual TETRA network.

Summary of the invention

An object of the invention is to overcome or alleviate the authentication problems encountered in a dual network or in roaming between different networks.

5 These and other objects of the present invention will be achieved by the method and system as claimed in the attached independent claims.

In the present invention a radio access network infrastructure, called the radio access network infrastructure layer is connected to a second network infrastructure, called a second overlaying network infrastructure layer, 10 which has different authentication procedures and triplets than the radio access network. The radio access network may be for example a TETRA network which is connected via an A-interface to a network sub-system (NSS) of the GSM and thereby substitutes for the normal GSM base station sub-system (BSS). In the preferred embodiment of the invention the radio access network 15 layer and the overlaying network are combined into a single network called a dual network herein. As noted above, the dual network enables the introduction of new features into the TETRA network by using features as well as network elements already developed for other systems, such as the GSM or the UMTS.

20 In another embodiment of the invention the overlaying second network infrastructure layer is provided by the home network of a mobile station roaming in the radio access network.

The problem relating to the different authentication schemes is overcome by using the authentication of the overlaying network layer in combination with the authentication procedures of the radio access network layer. 25 When the mobile station first time registers to the system, the mobile station is first authenticated in the overlaying network layer. In this initial authentication the authentication procedures and authentication parameters of the overlaying network, such as the authentication triplet of the GSM, is used. The authentication parameters of the radio access layer, such as the random seed and the random challenge of the TETRA, are derived from the authentication parameters used in the initial authentication. Then the derived authentication parameters are used in any subsequent authentication procedure within the first 30 radio access infrastructure layer until new authentication is needed in the overlaying network infrastructure layer.

In the preferred embodiment of the invention one of the authentication parameters generated in the second network infrastructure layer and the mobile station during the initial authentication is a ciphering key. In accordance with the invention the second ciphering key for the radio access network infrastructure layer is derived from the first ciphering key and is used for ciphering the communication between the mobile station and the first network infrastructure layer.

As the radio access layer authentication parameters are derived from the overlaying layer authentication parameters by specific operations, the original overlaying layer parameters can be restored from the derived authentication parameter at any point within the radio access network. In a preferred embodiment, the overlaying network parameters are translated into appropriate radio access layer authentication parameters which are then transmitted to the mobile station with radio access network signaling, and required authentication parameter(s) will then be restored to the mobile station by an inverse operation and is (are) used by overlaying network layer authentication algorithms.

The present invention provides a number of advantages. For example in a dual TETRA network having the GSM as an overlaying network layer, the GSM-type authentication is possible both in GSM and TETRA networks, i.e. roaming from a dual TETRA to a GSM network, and vice versa, will be possible. Inside the dual TETRA network, standard TETRA authentication procedures (including mutual authentication) can be used. As standard TETRA authentication procedures are used in the TETRA layer, a conventional terminal having no GSM or dual TETRA related features will also work inside TETRA and dual TETRA networks according to the present invention.

Brief description of the drawings

In the following the invention will be described in more detail by means of preferred embodiments with reference to the attached drawings, wherein

Figure 1 illustrates the standard TETRA authentication of the user by the infrastructure,

Figure 2 illustrates the standard TETRA authentication of the infrastructure by a user,

Figure 3 illustrates the mutual authentication of the infrastructure and the user according to the TETRA standard,

Figure 4 illustrates a dual TETRA network and mobility scenario according to the present invention,

5 Figure 5 illustrates derivation of the TETRA authentication triplet from the GSM authentication triplet,

Figure 6 illustrates the initial GSM authentication in a dual TETRA network according to the invention, and

10 Figure 7 illustrates the second-phase TETRA authentication in the dual TETRA network according to the present invention.

Detailed description of the invention

Preferred embodiments of the invention will be described in the following as implemented in a dual TETRA network, i.e. the radio access network layer is TETRA and the overlaying second network layer is GSM, but the intention is not to restrict the invention to this concept.

20 Figure 4 illustrates the dual TETRA architecture. The TETRA network comprises digital exchanges DXT, to which the base stations TBS are connected. An original or a smaller nation-wide network is normally built around several DXT exchanges, which are interconnected by a central digital exchange for the TETRA (DXT_c), to form a two-layer star hierarchy and to provide resilient traffic routing and fast call set-up times. The TETRA utilizes a distributor subscriber data base structure so that there is a home location register (HLR) for the network's own subscribers and a visitor location register (VLR) for the visiting subscribers. Typically each DXT is provided with a VLR.

25 There is normally only one HLR which is located at one of the DXTs in the network (referred to as DXTh). Some of the DXTs (GW DXT) provide a gateway to other telecommunication networks. For connecting together different TETRA networks, an intersystem interface (ISI) is defined in the TETRA standard.

30 The TETRA layer also includes a TETRA-specific authentication center AuC for TETRA authentications. In Figure 4 the TETRA AuC is located in the DXTh. Therefore, the TETRA layer provides all standard features and services of the TETRA to the TETRA users and mobile stations.

35 In order to introduce new features and services, such as roaming to other networks, an overlaying GSM layer is provided. The canonical GSM architecture distinguishes two parts: the BSS (base station sub-system) and the

NSS (network and switching sub-system). The NSS includes the main switching functions of the GSM, as well as the data bases needed for subscriber data and mobility management. In the dual TETRA network, the GSM infrastructure layer is formed by a network and switching sub-system (NSS) of the

5 GSM which is connected via an A-interface to the TETRA. Thus, the TETRA network is used as a radio access network for the GSM NSS instead of a conventional GSM BSS. The A-interface may be connected to a DXT in the TETRA layer, as shown in Figure 4.

Within the GSM layer, the basic switching function is performed by

10 the MSC (mobile services switching center) whose main function is to coordinate the setting up of calls to and from the dual TETRA users (or GSM users). The MSC has interfaces with the TETRA layer on one side (through which it is in contact with the dual TETRA users), and with external networks on the other. The interface with external networks is for communication with

15 users outside the dual TETRA network. The interworking functions required for the interface to other networks may be concentrated in one of the MSCs, a gateway MSC (GW MSC). Besides MSCs, the GSM layer includes data bases, i.e. home location registers (HLR) and visitors location registers (VLR). Typically, the VLR function is integrated with each MSC. A functional part of the

20 HLR is the authentication center (AuC) managing the security data for the authentication of the subscribers.

This type of a dual TETRA network, i.e. a combination of TETRA and GSM networks, basically allows the subscriber to roam in the TETRA, dual TETRA and GSM networks, and enables the TETRA network to use at

25 least some of the GSM features and services. The mobility scenario includes several roaming possibilities. As illustrated in Figure 4, the subscriber of a dual TETRA network is able to roam (1) from a dual TETRA network A to a dual TETRA network B, and (2) from a dual TETRA network to a GSM network. Similarly, the subscriber of another network is able to roam (4) from a GSM

30 network to a dual TETRA network and (5) from a TETRA network to a dual TETRA network. The subscriber of the GSM network may have a dual mode terminal which is able to operate both in the GSM air interface and the TETRA air interface. Similarly, only a dual TETRA terminal which is able to operate both in the TETRA air interface and the GSM air interface is able to roam to a

35 GSM network. Also SIM roaming is possible; a dual TETRA SIM is used in GSM mobile equipment ME in a GSM network, or vice versa, a GSM SIM is

used in dual TETRA ME in a dual TETRA network. However, a dual TETRA terminal which is used only within the dual TETRA network does not necessarily require the GSM air interface capability: it only utilizes the new services provided by the GSM layer in the dual TETRA network. The conventional

5 TETRA terminal can operate both in a dual TETRA network and a standard TETRA network, but it is not able to utilize the services of the GSM layer in the dual TETRA network.

The authentication in the GSM differs from authentication in the TETRA. The security-related network functions of the GSM are defined in the

10 ETSI specification ETS300534 (GMS03.20 version 4.4.1) which is incorporated herein as a reference. The security functions of the TETRA are defined in the ETSI specification ETS300392-7 TETRA V+D; part 7: security, which is incorporated herein as a reference. In the GSM system, the MSC may request authentication parameters for each subscriber MS from the authentication

15 center AuC of the subscriber's MS home network. The AuC is either a separate unit or integrated into the HLR, as illustrated in Figure 4. Referring to Figure 6, the GSM AuC stores a secret authentication key Ki for each subscriber identity. In addition, the AuC generates one or more random challenge numbers RAND. A reference parameter SRES (the expected response) is derived

20 from the RAND and the key Ki by an authentication algorithm A3. Similarly, also an encryption key Kc is computed from the RAND and the Ki by a second authentication algorithm A8. The algorithms A3 and A8 are not specified in the ETSI standard but can be chosen by the network operator. The resulting authentication parameters, the RAND, the SRES and the Kc, are called a

25 GSM authentication triplet.

As noted above, the GSM authentication triplet differs from the authentication triplet (RS, KS, KS') provided by the DXTh/AuC and from the random challenge RAND1 derived by the DXT or the BS in the standard TETRA authentication procedures. Therefore, in accordance with the basic

30 principles of the present invention, the TETRA authentication triplet (RS, KS, KS'), the RAND1 and the encryption key DCK are derived from the GSM authentication triplet (RAND, SRES, Kc). In the preferred embodiment of the invention this derivation is implemented in the interface between the MSC/VLR and the DXT.

35 Figure 5 illustrates an example of derivation of the TETRA triplet (RS, KS, KS') from the GSM triplet.

The 80-bit Random Seed RS is derived by taking the leftmost 80 bits from the 128-bit RAND:

$$RS = LEFT(RAND, 80) \quad (1)$$

The 128-bit session authentication key KS is derived by concatenating the 64-bit Kc with a fixed 64-bit value FIXC (the Kc is preferably generated by a modified A8 algorithm, as will be described below):

$$KS = Kc + FIXC(64) \quad (2)$$

The 128-bit session authentication key KS' is derived by concatenating the 64-bit Kc with a fixed 64-bit value FIXC':

$$KS' = FIXC'(64) + Kc \quad (3)$$

Due to the derived TETRA parameters, standard TETRA authentication procedures can be used within the TETRA network layer. However, although a 128-bit RAND could be used in the GSM authentication, there are only 80 random bits (the Random Seed RS) available in the succeeding DTETRA authentication. As the KS and KS' will not be transferred over the air interface to the MS, the MS must derive KS and KS' using the secret key K and the RS. For this reason, in the preferred embodiment of the invention, modified authentication algorithms A8 are introduced into the DTETRA AuC in the GSM layer and the DTETRA SIM in the MS. The standard A8 implementation A8g can be presented as follows:

$$Kc[64] = A8g(Ki[128], RAND[128]) \quad (4)$$

wherein Ki and RAND are 128-bit values. The modified algorithm A8g used for calculating Kc in the DTETRA AuC may then be:

$$Kc = A8(Ki, RAND) = A8g(Ki, LEFT(RAND, 80) + FIXD(48)) \quad (5)$$

In other words, the new A8 algorithm has a 'preprocessor' that replaces 48 random bits of the 128-bit RAND with the constant 48 bits of FIXD. There are several ways to choose 80 bits out of 128 bits. They should be evaluated against the operation of the used A8g algorithm in order to find the best one. It should be noted that the selection and derivation methods presented here are only examples. In the above equation, the 80 leftmost bits are chosen. The modified algorithm A8s used for calculating Kc from the 80-bit RS in the DTETRA MS may then be:

$$Kc = A8s(K, RS[80]) = A8g(Ki, RS + FIXD(48)) \quad (6)$$

The MS can now derive KS and KS' using the secret key K and RS as follows

$$KS = Kc + FIXC(64) = A8s(K, RS) + FIXC(64) \quad (7)$$

$$KS' = \text{FIXC}'(64) + Kc = \text{FIXC}'(64) + A8s(K, RS) \quad (8)$$

Initial GSM authentication in DTETRA network

An example of an initial GSM authentication in a Dual TETRA

5 (DTETRA) network will now be described with reference to Figure 6. This is a simple case of transferring GSM authentication data over the TETRA infrastructure and the air interface AI. In the example case the subscriber of the MS is a DTETRA subscriber, and the MS is provided with a DTETRA subscriber identification module (SIM) instead of a TETRA SIM. The mobile terminal part ME of the MS may be a standard TETRA terminal.

10 1. The AuC has generated the GSM triplet (RAND, SRES, Kc) with the random generator and algorithms A3 and A8g, as described above.

15 2. The MSC/VLR obtains the GSM triplet from the AuC and requests authentication due to location update or call setup. The VLR sends (RAND, Kc) to the DXT. SRES is stored in the VLR.

16 3. The DXT sets the derived ciphering key DCK for TETRA:

$$DCK = Kc + \text{FIXA}(16) \quad (9)$$

20 In other words Kc is concatenated with a 16-bit constant FIXA (LSB bits).

25 5. The DXT derives the 80-bit Random Seed RS and the 80-bit Random Challenge RAND1:

$$RS = \text{LEFT}(RAND, 80) \quad (10)$$

$$RAND1 = \text{FIXB}(32) + \text{RIGHT}(RAND, 48) \quad (11)$$

26 In other words, RS is formed by the leftmost 80 bits (MSB) of RAND, and the remaining rightmost 48 bits (LSB) are concatenated with a 32-bit constant FIXB (MSB-bits) so as to form RAND1.

30 6. The DXT sends a TETRA authentication request (RS, RAND1) to the MS.

31 7. The mobile equipment part ME of the MS sends RS and RAND1 to the Dual TETRA SIM (i.e. TSIM). The TSIM detects that the leftmost 32-bits of the received RAND1 contain the constant FIXB, i.e. $\text{LEFT}(RAND1, 32) = \text{FIXB}(32)$, and therefore uses GSM authentication algorithms.

8. The TSIM sets $RAND = RS + RIGHT(RAND1, 48)$, i.e. concatenates RS and the leftmost 48 bits of RAND1 in order to obtain the original RAND.
9. Then the SIM computes $DCK = Kc + FIXA(16) = A8s(K, RS) + FIXA(16)$ and $SRES = A3(K, RAND)$, and returns DCK and SRES to the ME.
10. The ME stores DCK and sends SRES to the DXT as RES1 (i.e. the TETRA parameter).
11. The DXT sends RES1 as SRES to the VLR.
12. The VLR compares the received SRES to the SRES from the GSM triplet, and accepts the authentication, if the SRES values match.
13. The DXT sends the authentication result R1 to the MS.

The steps 7 to 10 of the authentication process in the ME and the SIM will be different, if the ME is provided with a GSM SIM (GSIM), e.g. a GSM subscriber is visiting the DTETRA network. In that case the ME has to have additional dual TETRA functionality. The modified steps 7' to 10' are:

- 7'. The ME knows the SIM type, and so computes $RAND = RS + RIGHT(RAND1, 48)$, i.e. concatenates RS and the leftmost 48 bits of RAND1 in order to obtain the original.
- 8'. The ME sends RAND to the GSIM.
- 9'. Then the GSIM computes $Kc = A8(Ki, RAND)$ and $SRES = A3(Ki, RAND)$, and sends them to the ME.
- 10'. The ME sets $DCK = Kc + FIXA(16)$, stores DCK and sends SRES to the DXT as RES1 (i.e. the TETRA parameter).

DTETRA authentication based on preceding GSM authentication

The TETRA authentication, such as the one described with reference to Figure 2 or 3, may be used when the transactions stay inside the DTETRA network. It is assumed that only ME + TSIM may participate in these transactions, so the AuC that issued the original GSM triplet has special DTETRA algorithms, as described above. An example of how to use the GSM triplet in the 2nd phase of TETRA authentication will be described in the following with reference to Figure 7.

1. The DXT cannot calculate the session authentication key KS , because it does not know the TETRA authentication key K . Therefore, the DXT uses information from the preceding GSM authentication in the calculation. In accordance with the equations (7), (8) and (1):
5 $KS = Kc + FIXC(64)$; $KS' = FIXC'(64) + Kc$; and $RS = LEFT(RAND, 80)$. The DXT also generates a random challenge $RAND1 = \text{random}$. It should be checked that $LEFT(RAND1, 32)$ is not equal to $FIXB(32)$ in order to avoid misinterpretation in the TSIM.
- 10 2. The DXT computes the expected response and the ciphering key by the TA12 algorithm in accordance with the TETRA standard
$$XRES1, DCK1 = TA12(KS, RAND1) \quad (12)$$
Also $XRES1$ and $DCK1$ are computed by the algorithm TA12. In case of KS' or mutual authentication, $RES2$ and $DCK2$ are calculated by the algorithm TA22. In the mutual authentication the final ciphering key is calculated by the algorithm TB4.
15 3. The DXT sends $(RS, RAND1)$ pair to the MS, where the ME forwards them to the TSIM.
4. The TSIM notices that $LEFT(RAND1, 32) \leftrightarrow FIXB(32)$, and consequently uses the TETRA authentication algorithms.
20 5. In the TSIM a special TA11 algorithm that uses the A8s algorithm is used for computing KS :
$$KS = TA11(K, RS) = A8s(K, RS) + FIXC(64) \quad (13)$$
Similarly, if the session key KS' is needed, it is computed by a special TA21 algorithm that uses the A8s algorithm:
25
$$KS' = TA21(K, RS) = FIXC'(64) + A8s(K, RS) \quad (14)$$
 KS' is needed when the MS tries to authenticate the network, or in mutual authentication.
6. The response $RES1$ and $DCK1$ are computed with the algorithm TA12
30
$$RES1, DCK1 = TA12(KS, RAND1) \quad (15)$$
In case of KS' or mutual authentication, $XRES2$ and $DCK2$ are calculated by the algorithm TA22. In the mutual authentication the final ciphering key is calculated by the algorithm TB4.
7. The MS sends $RES1$ to the DXT which compares $RES1$ to $XRES1$. If the values match, the authentication is accepted.
35 8. The DXT sends the authentication result $R1$ to the MS.

Standard TETRA authentication

If the DXT receives a TETRA authentication triplet (RS, KS, KS') (see Figure 7, Tetra layer), then it will use standard TETRA algorithms. The 5 DTETRA SIM is not used in this case, since DTETRA AuC does not send TETRA authentication triplets.

GSM authentication in GSM network

If the ME with DTETRA SIM roams to a GSM network, then the authentication triplet is asked from DTETRA AuC. The SIM receives RAND and returns SRES and Kc. 10

The description only illustrates preferred embodiments of the invention. The invention is not, however, limited to these embodiments but it may vary within the scope and the spirit of the appended claims.

Claims

1. An authentication method in a mobile communications system comprising a first radio access network infrastructure layer having first authentication procedures and first authentication parameters, and a second overlaying network infrastructure layer having second authentication procedures and second authentication parameters, characterized by steps of
 - 5 performing the initial authentication of a mobile station with the second authentication procedures and the second authentication parameters in order to authenticate the mobile station in the overlaying second network infrastructure layer,
 - 10 deriving the first authentication parameters for the first radio access network infrastructure layer from said second authentication parameters during said initial authentication,
 - 15 using said derived first authentication parameters for any subsequent authentication in the first radio access infrastructure layer until the next initial authentication in the overlaying second overlaying network infrastructure layer.
2. A method as claimed in claim 1, characterized by steps of
 - 20 generating a first ciphering key for the overlaying second network infrastructure layer during said initial authentication in the second network infrastructure layer and the mobile station,
 - 25 deriving a second ciphering key for the radio access network infrastructure layer from said first ciphering key in the first network infrastructure layer and the mobile station,
 - 30 using said second ciphering key for ciphering a communication between the mobile station and the first network infrastructure layer.
3. A method as claimed in claim 1 or 2, characterized by steps of
 - 35 transferring, in accordance with said first authentication procedures, one or more of said derived first authentication parameters to the mobile station during said initial authentication,
 - 40 restoring at least one of said second authentication parameters from said one or more derived first authentication parameters received in order to enable said initial authentication in the mobile station.
- 35 4. A method as claimed in claim 1, 2 or 3, characterized by steps of

deriving one or more session authentication keys from a secret authentication key in the first radio access network infrastructure layer and the mobile station, said one or more session authentication keys being used in said further authentications in the first radio access network infrastructure 5 layer.

5. A method as claimed in claim 4, characterized by one or more session authentication keys being used for generating further authentication parameters in said further authentications.

6. A method as claimed in claim 1, 2, 3, 4 or 5, characterized 10 by steps of

generating a random challenge number in the second overlaying network infrastructure layer,

computing an expected response from said random challenge number and a secret authentication key by a first authentication algorithm in 15 the second overlaying network infrastructure layer,

computing a first ciphering key from said random challenge number and said secret authentication key by a second authentication algorithm in the second overlaying network infrastructure layer,

forwarding said random challenge number and said ciphering key to 20 the first radio access network infrastructure layer,

translating the random challenge number into one or more authentication parameters of the first infrastructure layer,

deriving a ciphering key for the first network infrastructure layer from said first ciphering key,

25 sending said one or more translated authentication parameters carrying the random challenge number to a mobile station in accordance with the authentication procedures of the first infrastructure layer,

restoring said random challenge number from said one or more translated authentication parameters,

30 computing a response and said first ciphering key from said random challenge number and said secret authentication key by said first and respectively second authentication algorithms in the mobile station,

deriving a second ciphering key for the first network infrastructure layer from said first ciphering key in the mobile station,

35 sending the response to the second network infrastructure layer to be authenticated by comparing with said expected response,

using said one or more translated authentication parameters and said derived ciphering key in any further authentication procedure and ciphering procedure in the first network infrastructure layer until the next initial authentication in the second network layer.

5 7. A method as claimed in claim 6, characterized in that
 said step of translating said random challenge comprises a step of
 1) forming an 80-bit random seed from selected 80 bits of the 128-bit random
 challenge, and 2) combining the remaining 48 bits of the 128-bit random chal-
 lenge with a predetermined 32-bit constant in order to provide an 80-bit ran-
10 dom challenge,

 said step of restoring said random challenge comprises steps of
 extracting the 48 bits from the 80-bit random challenge, and combining said
 extracted bits with said 80-bit random seed in order to provide said 128-bit
 random challenge.

15 8. A method as claimed in claim 6 or 7, characterized in that
 said steps of deriving the second ciphering key comprises step of combining
 predetermined additional 16 bits to the 64-bit first ciphering key in order to
 provide the 80-bit second ciphering key.

16 9. A method as claimed in any one of claims 1 to 8, charac-
20 terized in that said second network infrastructure layer is part of another
 network from which the mobile station is visiting in the first radio-access radio
 network.

25 10. A method as claimed in any one of claims 1 to 8, charac-
 terized in that said first network infrastructure layer is a TETRA-type net-
 work.

30 11. A mobile communications system comprising a first radio ac-
 cess network infrastructure layer (TETRA) having first authentication pro-
 cedures and first authentication parameters (RS,RAND1,KS,KS',DCK), and a
 second overlaying network infrastructure layer (GSM) having second authenti-
 cation procedures and second authentication parameters (RAND,SRES,Kc),
 characterized by the system being arranged to

35 perform the initial authentication of a mobile station (MS) with the
 second authentication procedures and the second authentication parameters
 (RAND,SRES,Kc) in order to authenticate the mobile station (MS) in the over-
 laying second network infrastructure layer (GSM),

derive the first authentication parameters (RS,RAND1,KS,KS',DCK) for the first radio access network infrastructure layer (TETRA) from said second authentication parameters (RAND,SRES,Kc) during said initial authentication,

5 use said derived first authentication parameters (RS,RAND1,KS,KS',DCK) for any subsequent authentication in the first radio access infrastructure layer (TETRA) until the next initial authentication in the overlaying second network infrastructure layer (GSM).

12. A system as claimed in claim 11, characterized by

10 the second network infrastructure layer (GSM) and the mobile station (MS) being arranged to generate a first ciphering key (Kc) for the overlaying second network infrastructure layer during said initial authentication in the second network infrastructure layer (GSM) and the mobile station (MS),

the first network infrastructure layer (TETRA) and the mobile station

15 (MS) being arranged to derive a second ciphering key (DCK) for the radio access network infrastructure layer from said first ciphering key (Kc),

the first network infrastructure layer (TETRA) and the mobile station (MS) being arranged to use said second ciphering key (DCK) for ciphering a communication between the mobile station and the first network infrastructure

20 layer.

13. A system as claimed in claim 11 or 12, characterized by

the first network infrastructure layer (TETRA) being arranged to transfer one or more of said derived first authentication parameters (RS,RAND1) to the mobile station (MS) during said initial authentication,

25 the mobile station (MS) being arranged to restore at least one of said second authentication parameters (RAND) from said one or more derived first authentication parameters received in order to enable said initial authentication.

14. A system as claimed in claim 11, 12 or 13, characterized

30 by

the first radio access network infrastructure layer (TETRA) and the mobile station (MS) being arranged to derive one or more session authentication keys (KS,KS') from said first secret authentication key (Kc) in order to be used in said further authentications in the first radio access network infrastructure layer (TETRA).

15. A system as claimed in claim 14, characterized by the first radio access network infrastructure layer (TETRA) and the mobile station (MS) being arranged to use one or more session authentication keys (KS,KS') for generating further authentication parameters (RES1,XRES1) in said further 5 authentications.

16. A mobile station for a mobile communications system comprising a first radio access network infrastructure layer (TETRA) having first authentication procedures and first authentication parameters (RS,RAND1,KS,KS', DCK), and a second overlaying network infrastructure 10 layer (GSM) having second authentication procedures and second authentication parameters (RAND,SRES,Kc), characterized by said mobile station being arranged to

receive one or more first authentication parameters (SS,RAND1) from the radio access network infrastructure (TETRA) during an initial authentication to the network,
15

derive one or more of the second authentication parameters (RAND) from said received one or more of the first parameters,

compute a first ciphering key (Kc) and a response (SRES) from said derived one or more second authentication parameters (RAND) by authentication 20 algorithms (A3,A8s) of the overlaying network authentication procedures,

derive a second ciphering key (DCK) for the radio access network layer ciphering from said first ciphering key (Kc),

send said computed response (SRES) to the network infrastructure.

17. A mobile station according to claim 16, characterized in 25 that said mobile station is arranged to

derive one or more session authentication keys (KS,KS') from said first ciphering key (Kc),

use said derived one or more session authentication keys (KS,KS') in any first authentication procedures subsequent to the initial authentication.

30 18. A method for authentication of a mobile subscriber roaming in a first radio access network having first authentication procedures and first authentication parameters, from a second network having second authentication procedures and second authentication parameters, characterized by steps of

35 performing the initial authentication of a mobile station of the mobile subscriber using the second authentication procedures and the second

authentication parameters in order to authenticate the mobile station with the second network,

5 deriving the first authentication parameters for the first radio access network from said second authentication parameters during said initial authentication,

transferring one or more of said derived first parameters to the mobile station over the air interface,

10 restoring one or more of said second authentication parameters to the mobile station in order to enable the use of authentication algorithms according to said second authentication procedures,

sending an authentication response according to said second authentication procedures from the mobile station to the radio access network with signalling according to said first authentication procedures.

19. A method according to claim 18, characterized by steps

15 of

deriving a ciphering key used in the communication between the mobile station and the radio access network from one or more of said second authentication parameters,

20 using said derived first authentication parameters for any subsequent authentication in the first radio access infrastructure layer until the next initial authentication in the overlaying second overlaying network infrastructure layer.

25 20. An authentication method in a mobile communications system comprising a first radio access network infrastructure layer having first authentication procedures and first authentication parameters, and a second overlaying network infrastructure layer having second authentication procedures and second authentication parameters, characterized by steps of

30 performing the initial authentication of a mobile station with the second authentication procedures and the second authentication parameters in order to authenticate the mobile station in the overlaying second network infrastructure layer,

35 deriving the first authentication parameters for the first radio access network from said second authentication parameters during said initial authentication,

transferring one or more of said derived first parameters to the mobile station over the air interface,

restoring one or more of said second authentication parameters to the mobile station in order to enable the use of authentication algorithms according to said second authentication procedures,

5 sending an authentication response according to said second authentication procedures from the mobile station to the radio access network with signalling according to said first authentication procedures.

21. A method according to claim 20, characterized by steps of

10 using said derived first authentication parameters for any subsequent authentication in the first radio access infrastructure layer until the next initial authentication in the overlaying second overlaying network infrastructure layer.

22. A method according to claim 20 or 21, characterized by steps of

15 deriving a ciphering key used in the communication between the mobile station and the radio access network from one or more of said second authentication parameters.

23. A mobile communications system comprising a first radio access network infrastructure layer (TETRA) having first authentication procedures and first authentication parameters (RS,RAND1,KS,KS',DCK), and a second overlaying network infrastructure layer (GSM) having second authentication procedures and second authentication parameters (RAND,SRES,Kc), characterized by the system being arranged to

25 perform the initial authentication of a mobile station with the second authentication procedures and the second authentication parameters (RAND, SRES,Kc) in order to authenticate the mobile station (MS) in the overlaying second network infrastructure layer (GSM),

30 derive the first authentication parameters (RS,RAND1,KS,KS',DCK) for the first radio access network (TETRA) from said second authentication parameters (RAND,SRES,Kc) during said initial authentication,

transfer one or more of said derived first parameters (RS,RAND1) to the mobile station over the air interface,

35 restore one or more of said second authentication parameters (RAND) to the mobile station in order to enable the use of authentication algorithms (A3,A8s) according to said second authentication procedures,

send an authentication response (SRES) according to said second authentication procedures from the mobile station (MS) to the radio access network (TETRA) with signalling according to said first authentication procedures.

5 24. A system according to claim 23, characterized by the system being arranged to

use said derived first authentication parameters for any subsequent authentication in the first radio access infrastructure layer (TETRA) until the next initial authentication in the overlaying second overlaying network infrastructure layer (GSM).

10 25. A system according to claim 23 or 24, characterized by the system being arranged to

derive a ciphering key (DCK) used in the communication between the mobile station (MS) and the radio access network (TETRA) from one or 15 more of said second authentication parameters (Kc).

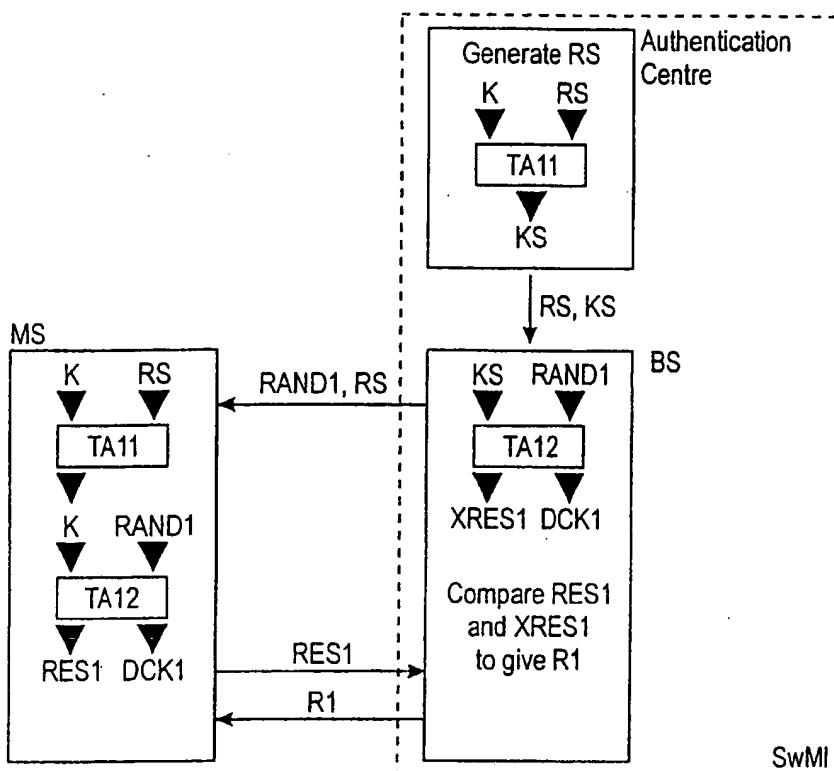


Fig. 1

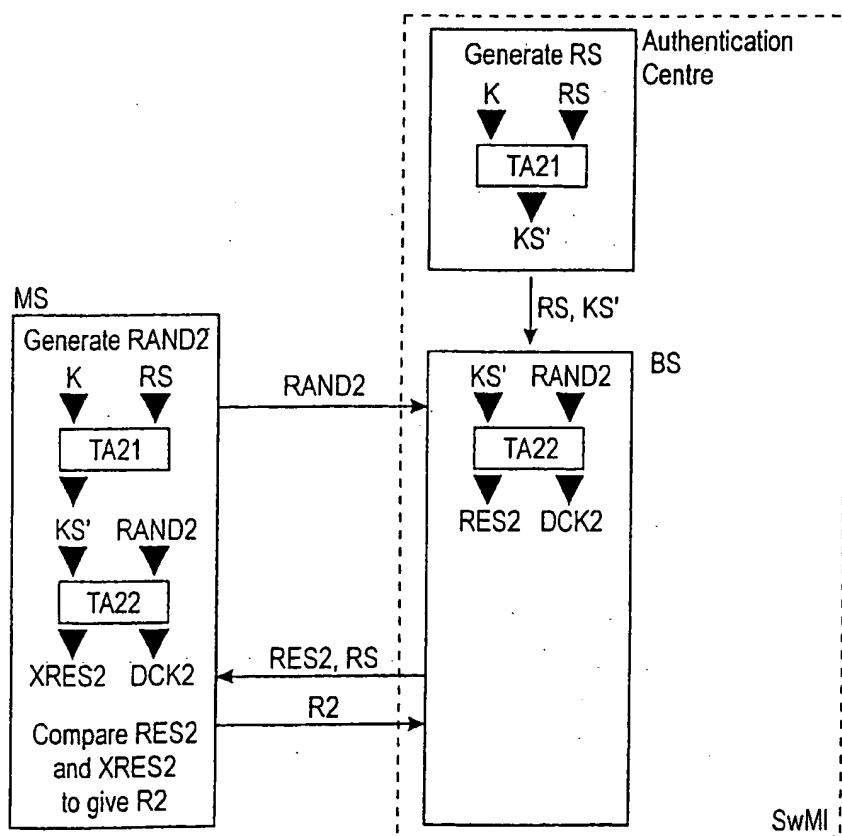


Fig. 2

2/4

Fig. 3

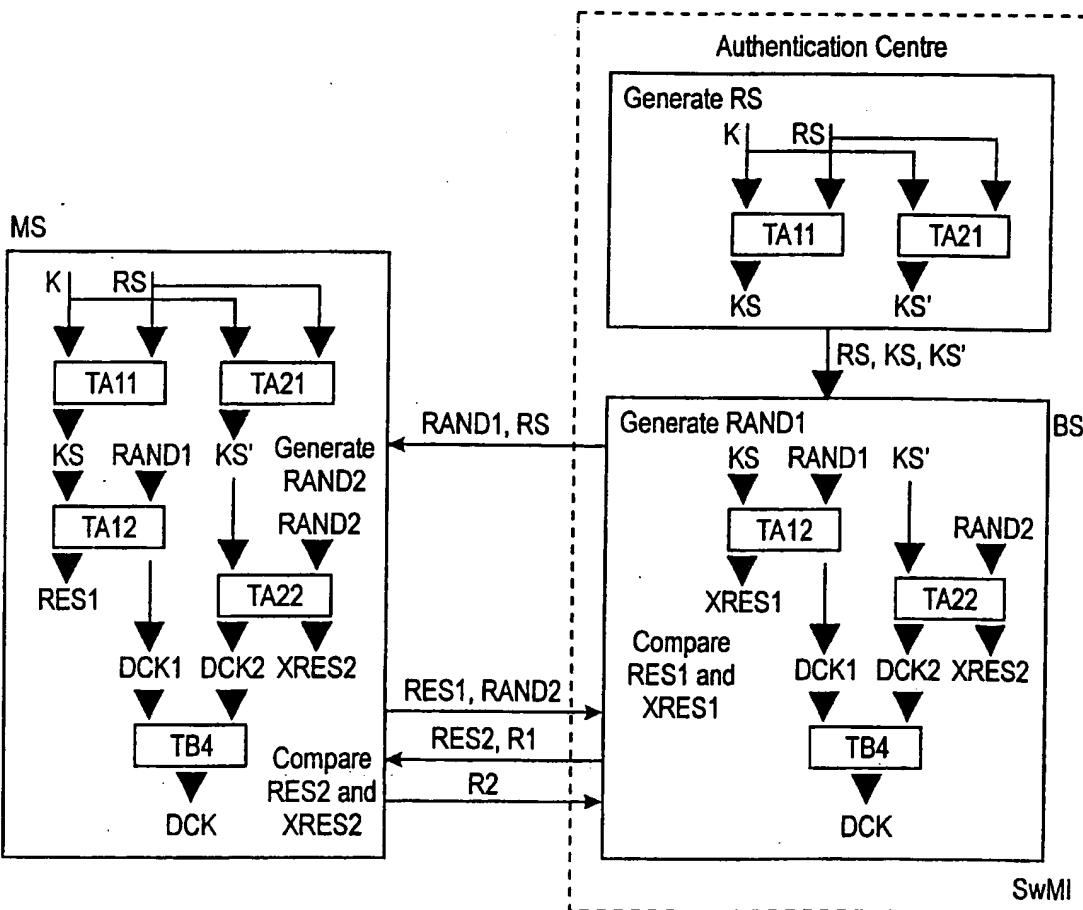


Fig. 4

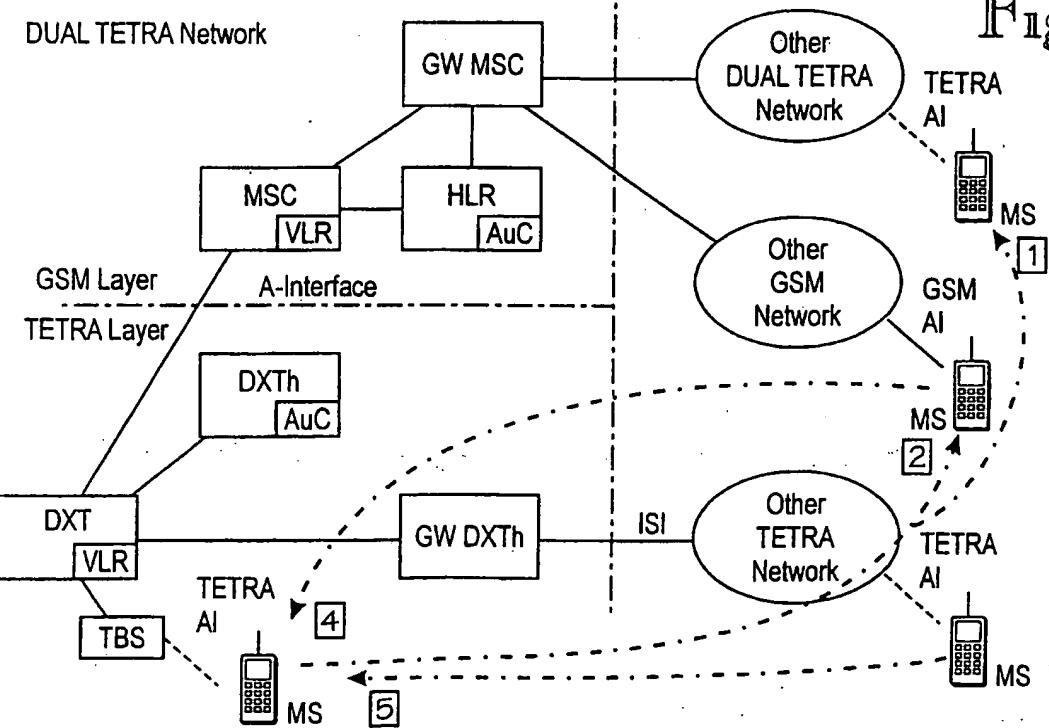


Fig. 5

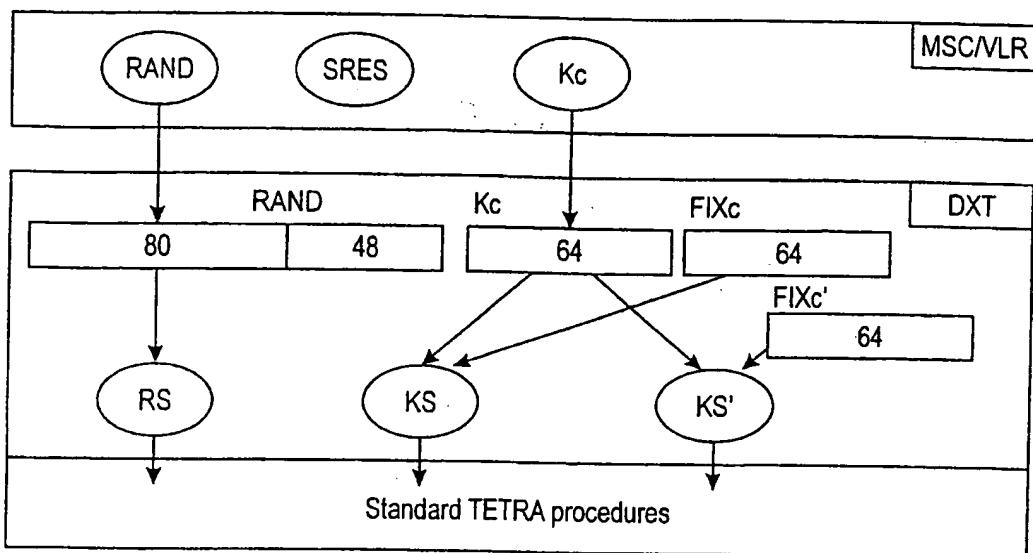


Fig. 7

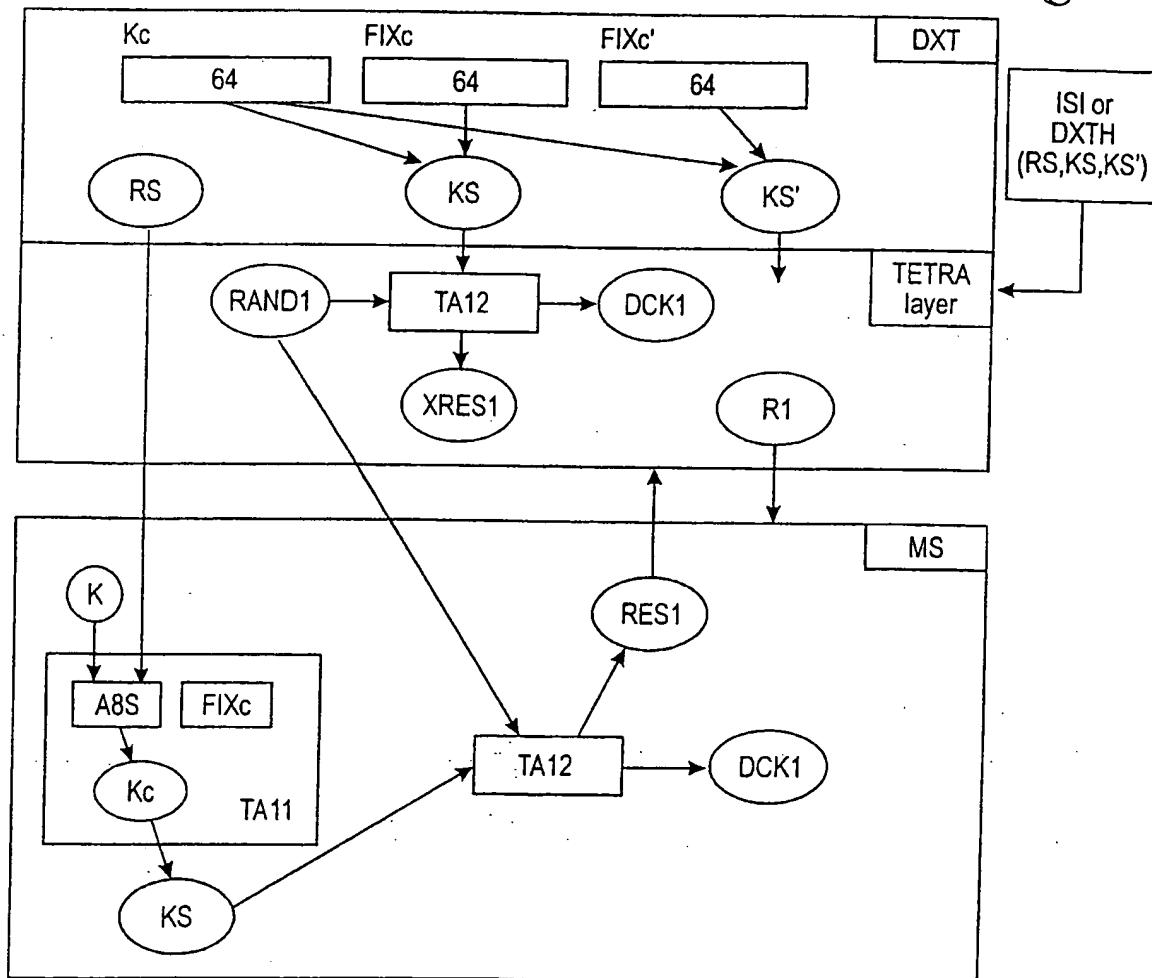
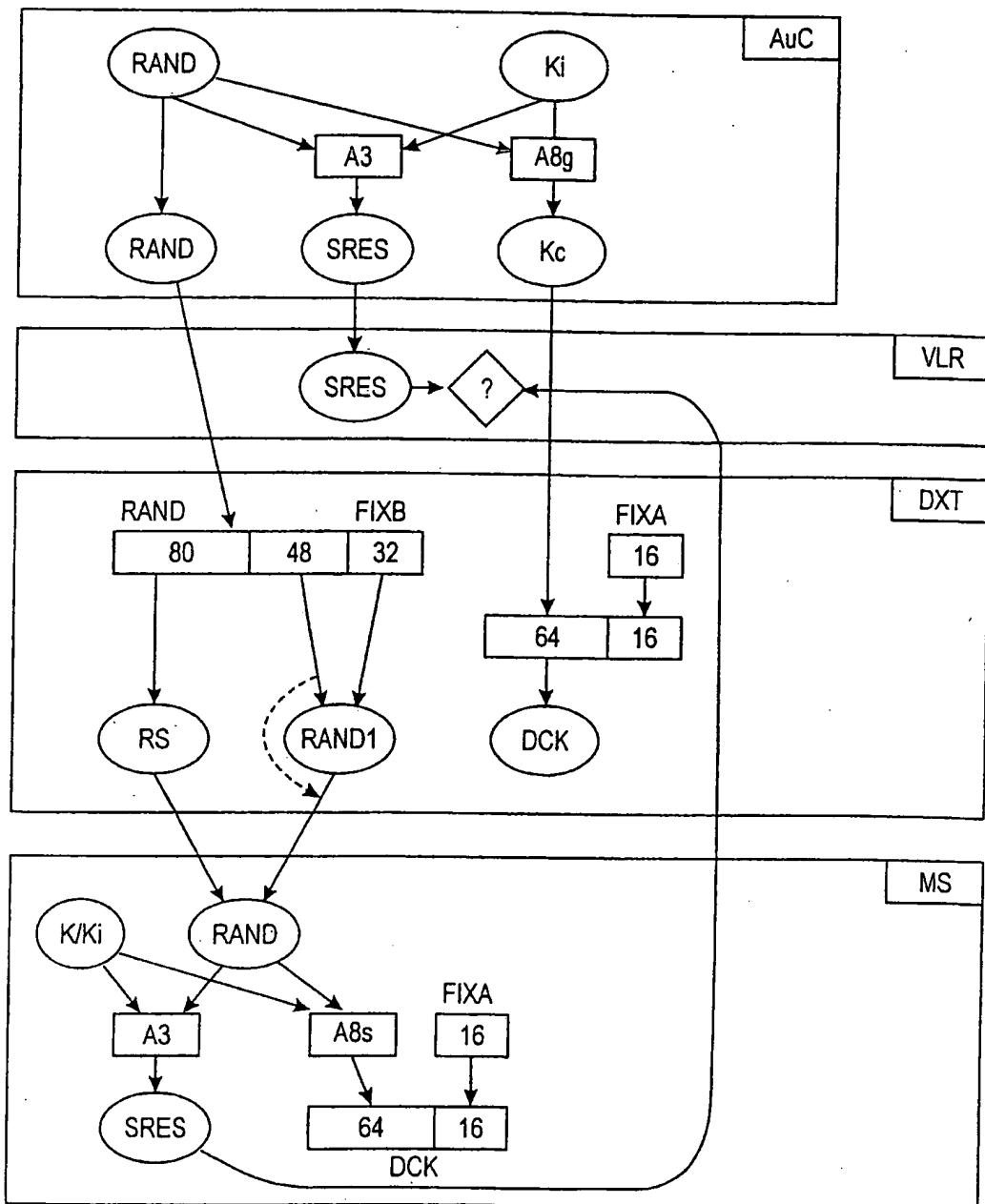


Fig. 6



INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00691

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04Q 7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9715161 A1 (NOKIA TELECOMMUNICATIONS OY), 24 April 1997 (24.04.97), page 5, line 1 - page 6, line 25; page 12, line 11 - page 14, line 13 --	1-25
P,A	EP 0955783 A2 (LUCENT TECHNOLOGIES INC.), 10 November 1999 (10.11.99), column 5, line 28 - column 6, line 24 --	1-25
A	WO 9605702 A2 (MOTOROLA INC.), 22 February 1996 (22.02.96), page 8, line 15 - page 11, line 20 --	1-25

 Further documents are listed in the continuation of Box C. See patent family annex.

- Special categories of cited documents:
- “A” document defining the general state of the art which is not considered to be of particular relevance
- “B” earlier application or patent but published on or after the international filing date
- “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- “O” document referring to an oral disclosure, use, exhibition or other means
- “P” document published prior to the international filing date but later than the priority date claimed
- “T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- “X” document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- “Y” document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- “&” document member of the same patent family

Date of the actual completion of the international search <u>21 November 2000</u>	Date of mailing of the international search report <u>23-11-2000</u>
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer <u>Jaana Raivio/JAn</u> Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00691

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0673178 A2 (KOKUSAI DENSHIN DENWA CO., LTD.), 20 Sept 1995 (20.09.95), column 2, line 23 - column 5, line 52 --	1-25
A	WO 9317529 A1 (NOKIA TELECOMMUNICATIONS OY), 2 Sept 1993 (02.09.93), page 3, line 23 - page 5, line 21 -----	1-25

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/FI 00/00691

Patent document cited in search report		Publication date	Patent family member(s)		Publication date	
WO	9715161	A1	24/04/97	AU CA EP JP US	7299196 A 2234655 A 0856233 A 11513853 T 5991407 A	07/05/97 24/04/97 05/08/98 24/11/99 23/11/99
EP	0955783	A2	10/11/99	AU BR CN JP	2696199 A 9901397 A 1259811 A 2000013873 A	18/11/99 18/01/00 12/07/00 14/01/00
WO	9605702	A2	22/02/96	BR CA EP FI JP KR US US	9506293 A 2171017 A 0721718 A 961404 A 9503895 T 227301 B 5537474 A 5668875 A	11/11/97 22/02/96 17/07/96 28/03/96 15/04/97 01/11/99 16/07/96 16/09/97
EP	0673178	A2	20/09/95	JP JP US JP	3047727 B 7264668 A 5596641 A 7307982 A	05/06/00 13/10/95 21/01/97 21/11/95
WO	9317529	A1	02/09/93	AT AU AU DE EP SE ES FI FI JP NO US	153207 T 657396 B 3501793 A 69310633 D,T 0583452 A,B 0583452 T3 2102640 T 90181 B,C 920792 D 6507293 T 933808 A 5557654 A	15/05/97 09/03/95 13/09/93 16/10/97 23/02/94 01/08/97 15/09/93 00/00/00 11/08/94 22/10/93 17/09/96